China International Strategy Review (2021) 3:97–114
https://doi.org/10.1007/s42533-021-00079-7

ORIGINAL PAPER

China–U.S. cyber-crisis management

Manshu XU[1] · **Chuanying LU**[1]

Received: 7 March 2021 / Accepted: 22 June 2021 / Published online: 28 June 2021

Abstract
In the past decade, cyber security issues have led to multiple conflicts between China and the United States, resulting in significant risks and threats to the cooperation of the two countries in cyberspace. Despite early successes and failures, cyber-crisis management is still in its infancy. Challenges, such as the misreading of cyberspace strategic intentions and the ideologization of technology competition, are very real. In the future, the two sides need to work together to seek consensus on the basic principles of crisis management, emphasize the important role of academic exchanges, and take confidence-building measures to lay the foundation for cooperation in cyber-crisis management.

Keywords Cyber security · China–U.S. relations · Crisis management

1 Preface: understanding cyber-crisis management

Since the 1990s, the application of the Internet and information and communication technology (ICT) has expanded rapidly, shaping a new space for human activities. In this virtual space, state-to-state rivalries have repeatedly arisen and have become the norm. Though they are generally low-intensity and involve limited confrontation, the danger of these tensions increasing or even escalating to full-scale confrontation triggered by cyberspace conflicts between countries is on the rise.

As cyberspace has become an important variable influencing international relations, it has also increasingly become a new area of international competition. Cyber-crisis management is often "integrated in the general crisis management structures, policies and plans—both nationally and internationally" (Trimintzios et al. 2014, 10). In international studies, the object of crisis management usually

✉ Manshu XU
xumanshu@hotmail.com

Chuanying LU
luchuanying@siis.org.cn

[1] Center for International Cyberspace Governance, Shanghai Institutes for International Studies, Shanghai, China

refers to international crises; that is, "a confrontation of two or more states, usually occupying a short time period, in which the probability of an outbreak of war between the participants is perceived to increase significantly" (Williams 1976, 25) and crisis management is often defined "in terms of restraint, i.e., measures to reduce the risk of war in a crisis" (Winham 1988, 15). In other words, crisis management is the combined use of diplomatic, military, and economic tools to control and manage crisis. The goal is to prevent a crisis from spinning out of control or leading to warfare and to seek peaceful solutions while protecting major national interests.

The subject of cyber-crisis management is the fierce competition and confrontation between countries in cyberspace. Although "cyber warfare" is often reported in the press, cyberattacks do not directly cause casualties and damage, so even military operations in cyberspace are within the scope of conflict, below the threshold of war. As a result, the conflict intensity presented by the confrontation between countries in cyberspace is relatively low, far from reaching the point when war is imminent. Although not strictly defined as an international crisis, such confrontations in cyberspace could exacerbate tensions between nations, leading to full-scale confrontation and even war.

First, low-intensity, frequent, malicious cyber actions can exacerbate suspicions, distrust, and security dilemmas among nations. On the one hand, with the rapid development and application of ICT, cyberspace is closely linked with national economy, social governance, and national security, with cybersecurity playing a leading role in national security. On the other hand, states and non-state actors, through cyberspace, have the capacity to directly or indirectly harm the prosperity, security, and vital values of other countries. In addition, the large number of non-state actors in cyberspace, the low cost of entry, the rapid diffusion of technologies, and the difficulty of attribution make it difficult to determine whether a cyberattack originating from a country is intentional, acquiescent, or poorly monitored. Nor can the attacker be held accountable on the basis of international law.

Second, low-intensity cyberspace operations can achieve strategic goals that harm the interests of other countries, causing sudden tensions between countries. In the contest between states, cyber tactics combine with political intent. For example, information online can affect the outcome of elections, and cyberattacks can disrupt the operation of underground nuclear facilities. By disrupting the enemy's information systems for critical national infrastructure, such as the economy, communications, and transportation, cyberattacks can provide even more lethal capabilities than missiles.

Third, military operations in cyberspace increase the risk of triggering real-world wars. Militarily, the greatest advantage of cyberspace operations is the ability to project force without the need to establish a physical presence in foreign territory (U.S. Joint Chiefs of Staff 2018, XII). Compared with the traditional military operations, military operations in cyberspace are more diverse, covert, and flexible, and it is easier to remotely manipulate adversaries' targets in cyberspace by means of deception, redirection, and system setting. This not only increases the fog of war, but also lowers the threshold for the use of military force.

In short, the emergence of cyberspace provides a new setting for confrontation between states. Cyber intelligence collection, critical infrastructure attacks, information influence operations, and cyberspace operations have become the main modes of action for countries to confront in cyberspace. With the cycle of attack and retaliation, the consequences of escalating, spillover, and spiraling out of control in cyberspace may be beyond the control of politicians. If the core idea of crisis management is extended to the cyber domain, cyber-crisis management can be understood as controlling and dealing with cyber incidents that may cause tension between countries, armed conflict, or even war. The aim is to prevent the escalation and spillover of the confrontation between countries in cyberspace and to avoid war.

In practice, cyber-crisis management has become a new agenda in the field of international arms control and has attracted the attention of some international organizations and academic research institutions. For example, the United Nations Institute for Disarmament Research (UNIDIR) has established a "cyber stability" project and organized an annual conference on strengthening crisis management in cyberspace. The Center for Humanitarian Dialogue, which has focused on the impact of cyber security threats on international security since 2019, aims to develop confidence-building measures between adversaries in cyberspace and a global framework for cyber stability. The MIT Computer Science and Artificial Intelligence Lab launched the Cyber Military Stability Roundtable in 2016; the multilateral research project aims to bring together scholars, think tanks and government officials from the United States, China, Russia, and other countries to explore ways to reduce cyber risks and promote international peace and security through a 1.5-track workshop.

In general, cyber-crisis management is a new development in international crisis management and is viewed by the international community through the conventional lenses of international crisis management in terms of goals and means. It is similarly divided into phases, such as prevention, control, and mitigation. In the pre-crisis, crisis response, and post-crisis periods, it employs a variety of tools, including crisis prevention, confidence-building, arms control, negotiation and international mediation, crisis response, and recovery and reconstruction. However, the virtual nature, anonymity, and dual-use by military and civilians, as well as the low intensity and high frequency of cyber conflicts, have brought about significant changes in crisis management in cyberspace. The "expansion in terms of tasks and timelines and the increasing number of actors involved have made effective coordination of activities and instruments an urgent priority" (Mölling 2008).

This paper defines China–U.S. cyber-crisis management as the control and handling of cyber incidents that may trigger tensions, armed conflicts and even wars between China and the United States, with the aim of managing the cyberspace differences and reducing the cyber risk that could trigger a deterioration of bilateral relations, or even a full-scale confrontation between the two countries. By analyzing the practices and major challenges of China–U.S. cyber-crisis management, the author hopes to find feasible ways to reduce distrust in China–U.S. cyberspace relations and promote a more stable relationship between the two cyber powers.

2 Review of China–U.S. confrontations in cyberspace

In the early 1990s, President Bill Clinton launched the "Information Superhighway" program, and the Internet expanded globally. During the George W. Bush administration, U.S. cyberspace strategy focused on strengthening the protection of key infrastructure and examining cybersecurity from the perspective of domestic security. Since its official access to the Internet began in 1994, China started late in informatization efforts, but developed rapidly. By 2008, the number of Internet users in China surpassed that of the United States for the first time, ranking first in the world (CNNIC 2008). From the perspective of overall strength, because the United States leads the world in information technology and its industrial scale, there is an obvious gap between China and the United States in cyber strength. At the same time, the intersection of the two sides involved in cyberspace is small, and therefore, their conflicts in cyberspace are not acute.

During the Obama administration, there were more and more cyber-related issues in China–U.S. relations. The cyber disputes between China and the United States focus on cybersecurity censorship, cyber theft and other "behaviors" in cyberspace, which are specific measures or activities in cyberspace. Through diplomatic efforts, China and the United States have reached basic consensus, established a dialogue on cybersecurity, and stabilized bilateral relations.

When Secretary of State Hillary Clinton was in office, the United States emphasized "Internet freedom" and used the free flow of information to oppose other countries' public policies on the Internet. It "required other countries to open their markets to American companies and promote American Internet companies to the world" (Lu 2014, 57). In the same period, China's Internet entered the era of mobile Internet and "We-Media." When the social value of the Internet as a communication platform emerged, and the scale effect of the Internet became large enough to affect national security, China took necessary measures to regulate domestic Internet problems. For the United States, Internet is a platform for expanding free market commerce and free speech, and for information and economic exchanges; therefore, China's cyber censorship policy violates American values. The banning of Facebook and Twitter and the withdrawal of Google from China also reflect the differences in the two countries' views on Internet governance. Later, along with the United States security review and suppression of Huawei and other Chinese high-tech enterprises, the United States government, enterprises, media, and academia accused China of cyber theft against the United States, escalating tensions and at one point rising to the level of fierce competition between countries. Fortunately, the intense confrontation between the two countries over cyber espionage has been eased, thanks to direct efforts at the highest levels in China and the United States.

2.1 The Obama-era China–U.S. cyber espionage dispute is widely regarded as a successful case of crisis management

The dispute originated with the Mandiant Report in 2013. In February 2013, U.S. company Mandiant claimed that the Chinese army was directly involved in hacking U.S. businesses, government, and critical infrastructure (Finkle 2013). This was the first-ever report on "cyber espionage" that named China as a sponsor. In June of the same year, "Prism Gate" revealed evidence showing U.S. intelligence agencies carrying out sustained, large-scale Internet surveillance on China, which in part motivated Chinese policymakers introduced a number of regulations designed to reduce dependence on foreign suppliers for critical technologies (Segal 2015). However, with the strategic consensus on building a new type of relationship (Campbell and Murray 2013), the two heads of state held their first dialogue on cyber security on June 8, 2013, and the cyber issue was thus incorporated into the Strategic and Economic Dialogue. In particular, under the Strategic Security Dialogue (SSD), the military departments of the two sides established the China–U.S. Cyber Working Group (CWG) in July 2013 and held the first meeting (Office of the Spokesperson of the United States 2013), which both sides considered the China–U.S. Cyber Working Group, the main platform for bilateral dialogue on cyber issues.

In 2014, the China–U.S. cyber espionage dispute began to escalate. In May 2014, the United States Department of Justice indicted five Chinese military officers for cyber theft. The Chinese Foreign Ministry responded angrily with unprecedented speed, demanding that the United States withdraw the case. Afterwards, the Chinese Foreign Ministry suspended the dialogue between the China–U.S. Cyber Security Working Group. At that moment, China–U.S. cyber relations fell to a freezing point. The dispute then came to a stalemate. The United States continues to smear China on cyber theft. Including, in June 2014, Cyber Security Company FireEye accused Unit 61,486 of continuing espionage against the U.S. and European industries (Menn 2014). In November 2014, *The Washington Post* said China hacked the United States National Oceanic and Atmospheric Administration and so on (Samenow and Rein 2014). The countermeasures taken by China include: in September 2014, the China Banking Regulatory Commission (CBRC) issued the "Guidance Opinions on Applying Secure and Controllable Information Technology to Strengthen the Construction of Banking Cybersecurity and Informatization"; In December 2014, the General Office of the China Banking Regulatory Commission and the General Office of the Ministry of Industry and Information Technology jointly issued the "Guide for Promoting the Application of Secure and Controllable Information Technology in the Banking Industry" (2014–2015), requiring Chinese financial institutions to improve the independent, controllable rate of information systems, so as to strengthen the construction of secure and controllable information technology and network security in the industry. A draft of China's proposed anti-terrorism law in March 2015 required foreign technology companies to hand over encryption keys for their products. In response, some U.S. officials and Western business groups argue that China's anti-terrorism law, including new banking regulations, puts unfair regulatory pressure on foreign companies (Blanchard 2015).

In 2015, the China–U.S. cyber espionage dispute continued to worsen. In April, FireEye revealed APT30, saying that China had been spying on governments and companies in Southeast Asian countries and India for a decade (FireEye Labs 2015). Subsequently, U.S. judicial action has escalated. On May 16, Zhang Hao, a professor at Tianjin University, was arrested while entering customs in Los Angeles and charged with economic espionage (Dunsmuir 2015). In late June, the U.S. Office of Personnel Management said its computer networks had been compromised, including the theft of Social Security numbers and other personal information from more than 21 million Americans. The United States government has linked the cyberattacks to China as retaliation against the United States. National Intelligence Director James Clapper identified China as the "leading suspect" in the attacks at a congressional hearing, adding that "[y]ou have to kind of salute the Chinese for what they did…. You know, if we had an opportunity to do that, I don't think we'd hesitate for a moment" (Finklea et al. 2015, 2). Shortly afterwards, United States media reported that Washington is considering sanctioning individuals or entities that benefit from cybertheft (Nakashima 2015). This was in the run-up to Chinese President Xi Jinping's planned visit to the country. Some in the United States called for the cancellation of the trip (Gass 2015). By this point, tensions surged in China–U.S. cyber relations.

Under the direct instructions of the two heads of state, the envoys of the two countries conducted urgent visits. U.S. National Security Adviser Condoleezza Rice visited China on August 30, during which the two sides discussed a range of sensitive issues, including cyber security, but officials from the two countries did not mention any differences over cyberattacks in front of reporters (Wong 2015). On September 9, President Xi Jinping's special envoy, a member of the Political Bureau of the CPC Central Committee and secretary of the CPC Central Political and Legal Commission, Meng Jianzhu, visited the United States. On September 11, the two sides announced that they had reached important consensus on prominent issues of cybersecurity (Reuters 2015). On the same day, U.S. President Barack Obama visited Fort Meade to give a speech. Obama said Chinese cyberattacks on the United States were "not acceptable and guarantee you we will win if we have to," but suggested "the two sides would have to agree on common rules in cyberspace" (BBC 2015). Then, on September 22, President Xi visited the United States. During his 4-day trip, he discussed the Internet four times, including a written interview with *The Wall Street Journal* (Ministry of Foreign Affairs of China 2015a), a welcome dinner in Seattle (Ministry of Foreign Affairs of China 2015b), a China–U.S. Internet Forum (Ministry of Foreign Affairs of China 2015c), and a meeting between the two heads of state (Ministry of Foreign Affairs of China 2015d). President Xi repeatedly stressed that China and the United States should cooperate, not confront.

Finally, on September 25, 2015, China and the United States reached six important consensuses on cybersecurity (Ministry of Foreign Affairs of China 2015e). Although China had previously rejected the distinction between acceptable national security spying and unacceptable economic espionage, the two sides reached a landmark agreement (Thomas 2016, 3), including that "states should not conduct or knowingly support misappropriation of intellectual property" and "ICT cyber security regulations should be consistent with WTO agreements." In addition, the two sides committed to cooperation

in sharing cybersecurity information, cybercrime investigations, and norms of state behavior in cyberspace.

It should be said that the successful management of this cyber crisis was directly attributable to the mediation of the heads of the two sides. Fundamentally, successful management is driven by China and the United States having a strategic need for each other on economic growth, regional stability, climate change and other major global affairs, as well as multilateral institutions. Chinese and U.S. policymakers appear committed to not letting cyber issues derail the U.S.–China relationship or interfere with cooperation on other high-profile issues (Tang and Segal 2016).

After the crisis eased, the two sides strengthened their cooperation, helping to get the cyber disputes between China and the United States under control in the late period of the Obama administration. First, China–U.S. high-level joint dialogue on combating cybercrimes and related issues has been established (U.S. Department of Justice 2015). Among the three dialogues from 2015 to 2017, the third joint dialogue was considered a milestone (U.S. Department of Justice 2016b) when the two sides agreed to establish a high-level expert group on cyber security to discuss international norms in cyberspace (U.S. Department of Justice 2016a), and launched China–U.S. hotline to crack down on cybercrime (U.S. Department of Justice 2016b). This mechanism enables China and the United States to have a working-level communication channel in the cyber domain. Second, a large number of cooperation projects have been signed between Chinese and American Internet enterprises, including Microsoft and China Electronic Technology's Windows 10 operating system project, Microsoft and Baidu's Windows 10 search engine project, Cisco and Inspur's cloud services project, EMC and Lenovo's data storage project, and Oracle and Tencent's database project. For China–U.S. cyberspace relations, the cooperation between Internet enterprises of the two sides has served as a ballast stone.

Under the Trump administration, the cyber dispute between China and the United States extended to the ICT industry, including related technologies, products, and services. At that time, China entered the era of the industrial Internet. The Chinese government calls for "informatization to drive modernization and build China into a cyber power" (Central Committee General Office of China 2016) and is committed to "promoting the deep integration of the Internet, big data, artificial intelligence and the real economy" (Xi 2017). As the Trump administration defined China as a "strategic competitor" and developed a competitive strategy in its dealings with China, the United States launched a trade war against China, while intensifying its crackdown on China in the field of science and technology, promoting "decoupling" from China's science, technology, and industry, and restricting China's high-tech development. China–U.S. competition was handled mainly by accusation, sanction, and confrontation.

2.2 China–U.S. conflicts in the ICT industry during the Trump administration should be regarded as a case of failed management

In 2018, the United States Department of Commerce adopted a number of economic sanctions against Chinese technologies and products, Internet companies, and tech companies producing products for civil and military purposes, citing national

security threats. The measures included export controls, import restrictions, wider investment reviews, revocation of licenses, and compelled selling.

After that, the United States blamed China for stealing trade secrets and forcing technology transfers to achieve technological innovation. Its response is a whole-of-government approach, which counters Chinese companies with a mix of economic, legal, diplomatic, and security tools. In November 2018, the Department of Justice launched the "China Initiative" to carry out law enforcement actions and investigations on Chinese companies and "cyber espionage behaviors," probe the extent to which the US high-tech industry was threatened by Chinese acquisitions, and assess supply chain security and the threats of "unregistered agents." In 2020, the United States government's expanded the Clean Network initiative, a stronger version of its 5G clean network initiative, and sought to restrict the overseas reach of Chinese Internet companies. The fight over ICT supply chain security is in essence a rivalry between industries and technologies in China and the United States. On the Chinese side, except for some counter measures taken by the Ministry of Foreign Affairs and Ministry of Commerce, China focused on increasing technology independence to enhance the security of industrial and supply chains.

The rising tensions between the two countries with regard to ICT supply chains heightens the sense of vulnerability on both sides. At same time, the United States made big adjustments to its cybersecurity strategy, introducing the highly aggressive strategy of persistent engagement and defense forward (U.S. Cyber Command 2018) and simplifying the approval procedure for offensive cyber operations of the Department of Defense by the National Defense Authorization Act for Fiscal Year 2019 and the 13th National Security Presidential Memorandum on the "U.S. Cyber Operations Policy" signed by Trump in August 2018. The situation increased the possibilities of cyber crisis and could take the two sides further toward the worst-case scenario.

From the perspective of crisis management and its principles, there are three reasons for the escalation of China–U.S. conflicts in the ICT industry. First, the two sides are strongly antagonistic to each other's strategic positioning. The Trump administration positioned China as a long-term strategic competitor that challenges American power, influence, and interests, and is attempting to erode American security and prosperity. The December 2017 National Security Strategy (NSS) and January 2018 National Defense Strategy (NDS) formally reoriented U.S. national security strategy and U.S. defense strategy toward an explicit primary focus on great power competition with China and Russia (Congressional Research Service 2021). U.S. concerns over Chinese military modernization, while China holds similar concerns over the United States' recent assessment that China is its primary security challenge both in a general sense and in cyberspace (Lyu 2019).

Second, cybersecurity was exaggerated. Trump administration bundled cybersecurity issues with economic, trade, technology, and even ideological issues, which were unprecedentedly magnified and politicized (Tang 2021). When cyber issues evolved into political issues, the resolution requires political will and an agenda. Regarding China as a prior rivalry of the United States, China–U.S. conflict in the ICT industry continued escalating with the extreme suppression tactics of the Trump administration. With the rapid deterioration of bilateral relations, cybersecurity was used as a starting

point for the Trump administration to launch trade wars and technological wars with China. Under such circumstances, it is difficult for the United States to find the will to control the escalation of the ICT conflict between China and the United States.

Third, communication channels were suspended. After Trump took office, China and the United States held the first round of law enforcement and cyber security dialogues on October 4, 2017. This continued the original high-level dialogue on matters related to combating cybercrime, but the United States believed that these discussions should not include issues such as cyberspace norms and ICT trade. With the deterioration of the China–U.S. relationship, the four high-level dialogue mechanisms, including the diplomatic and security dialogue, the comprehensive economic dialogue, the law enforcement and cyber security dialogues, and the social and people-to-people dialogue, were unilaterally interrupted by the Trump administration. Over 90 intergovernmental mechanisms (The White House 2013) between China and the United States were all in sleep mode, which increased the risk of miscalculation and escalation between the two sides.

To some degree, the ICT conflict between China and the United States is a crisis that is unlikely to be managed, because one side is determined to escalate the conflict. The deep reason lies in the fact that ICT "has become the primary source of geopolitical power" (Lynch III 2020, 139). With the accelerated integration of cyberspace and the real world, information and communication technologies have objectively become the main source of geopolitical power. This new power can shape the economy, critical civilian infrastructure, public opinion, and also military systems. As academics argue, "control over global telecommunications networks is a form of political power," (Doshi and McGuiness 2021, 1) and "the struggle for telecommunications standards can determine which states will wield network power" (Doshi and McGuiness 2021, 3). At the same time, strategic emerging technologies represented by ICT will continue to open up new ways of human productivity and life and give new impetus to economic development. Thus, the technological advantage will be transformed into a country's long-term economic advantage and military advantage. The 2021 final report to the United States Congress by the National Artificial Intelligence Security Council (NSCAI) states that "the magnitude of the technological opportunity coincides with a moment of strategic vulnerability. China is a competitor possessing the might, talent, and ambition to challenge America's technological leadership, military superiority, and its broader position in the world" (U.S. National Security Commission on Artificial Intelligence 2021, 19). When the United States believes that "In a number of critical technology areas—AI, quantum sciences, biotechnology—China is at a position of rough parity or has surpassed the United States" (Rasser and Lamberth 2021, 10), curbing the development of China's relevant technologies and industries is a natural choice for the United States to maintain its scientific and technological advantages.

3 Preview: main challenges on China–U.S. cyber-crisis management

How to deal with relations with China is a major challenge faced by the Biden administration. Given the strong bipartisan consensus on the growing "China threat", the Biden administration will carry on some elements of Trump's China

policy while returning to normal diplomatic practice. Due to the increasingly prominent strategic position and interest concerns on cybersecurity, increasing competition in the cyber domain between the two countries is inevitable, especially with the perception that "China's rise now profoundly impacts every major U.S. national interest" (The Atlantic Council 2021, 6). As "The superpower rivalry between the United States and China has also acquired a different, and possibly decisive, new dimension: cyber" (Thornhill 2020), cyberspace will undoubtedly become a major battleground for China–U.S. competition.

In the Obama era, the United States provoking the cyber espionage dispute against China reflects its response to the growth of China's cyber capabilities and, in particular, the comprehensive challenge that China's cyber power strategy may pose to the United States (Wang 2016, 102). Under Trump's presidency, China–U.S. cyber relations have been challenged by a number of factors, such as the trade war, technological blockade and the COVID-19 pandemic, and have presented a highly competitive and even confrontational posture. As cyber security remains high on President Biden's national security agenda, there will be "no radical departure from former President Trump's cyber policy in the next four years" and "competition will continue to be the defining feature of China–U.S. cyber interaction in the Biden administration, as it had been during the Trump term" (Chen and Lu 2021, 1).

Generally speaking, the China–U.S. cyberspace game will continue to revolve around the cyber intelligence struggle, key infrastructure attack and defense, information intervention, cyber force confrontation and international rulemaking. Meanwhile, since the competition of emerging technologies represented by ICT has become an important part of the strategic competition between China and the United States, the game between the two countries in cyberspace will be more reflected in the competition of science and technology around supply chain security, intellectual property protection, technical standard formulation, and ICT industry development. In terms of crisis management, China and the United States need to face strategic misunderstandings, politicization of disputes, communication failures, and other issues to prevent the China–U.S. cyberspace competition from leading to the deterioration of bilateral relations or even full-scale confrontation.

3.1 The first challenge is how to read each other's cyber strategy intentions

Cyber security is a new subject in China–U.S. relations; its complex nature and far-reaching implications make it difficult for both parties to read each other's strategic intentions through the conventional lenses of knowledge and cognition (Lu 2019). China prioritizes the Internet as an economic engine aiming to drive economic growth and boost the quality of growth by integrating emerging technology, whereas the United State perceives that, for example, China seeks to "leapfrog the United States as a technological power and thereby displace it as the world's dominant economic power" (The Atlantic Council 2021, 8) and "leverage emerging technologies to its national advantage in a way that disadvantages other nations" (Brannen et al. 2020).

Furthermore, China and the United States have very different military policies in cyberspace. China is opposed to cyberspace militarization and armament and stressed publicly the significance of cyber defense to national defense (The State Council Information Office of the People's Republic of China 2019, 14), whereas from the U.S. perspective, China is taking advantage of the asymmetrical feature of cyberspace to be ambiguous about and intentionally conceal its cyber capabilities to retain the possibility of sneak attacks on the United States. Its concern is that China may use cyberspace to target U.S. outer space assets and nuclear weaponry system, which could be a way of creating mutual deterrence similar to that in the nuclear field. The United States makes no secret of its having the "most mature and advanced military-cyber capabilities in the world" (King and Gallagher 2021, 10), whereas from the Chinese point of view, the United States' "transparency" in cyber military capabilities is a flaunting of power with the purpose to deter. The latest concepts of "defense forward" and "persistent engagement" indicate that the United States seeks to gain strategic advantage in combat capabilities through sustained confrontation with rivals and competitive cyber operations (Lu 2020). If the concept of "defense forward" is integrated into the broader U.S. cyber strategy, then more divergent perceptions, coupled with mutual distrust, will create major obstacles for cooperation in China–U.S. cyber-crisis management.

All these differences make it challenging for the two sides to read each other's strategic intentions and determine the strength of an actors' incentives for avoiding escalation and confrontation.

3.2 The second challenge is how to avoid the ideologization of technology competition

Technology competition between the United States and China is growing. As competition intensifies, the United States' approach to cyber issues is excessively ideological, with hacking, data security, and technology innovations all intricately linked to ideologies. And even the United States regards the differences in cyber governance as a reflection of different ideologies and development models. The Biden administration is also likely to retain and reinforce the restrictive measures against Chinese tech companies to push back against Beijing's so-called "digital authoritarianism" (Yayboke and Brannen 2020).

In theory, limitation of objectives pursued in the crisis, and limitation of means employed on behalf of those objectives are the two political requirements for crisis management (George 1991, 24). Ideologization may make each competitor feel that its fundamental interests were threatened on the one side. Although the two countries have not reached a point of direct confrontation in their strategic goals, the United States sees China as its top strategic rival, and China, albeit on strategic defense, will not concede or compromise on the most important issues. Should one side intentionally challenge the other on core interests, tensions will rise quickly.

On the other side, ideologization may cause one party to choose excessive actions in the context of dynamic interaction amidst a crisis. Cyber security is an interdisciplinary topic, where decision-making is complicated by the involvement of multiple

agencies. In handling cyber security incidents, those at the operational level play a key part. The bottom-up decision-making model is a far cry from the top-down approach usually taken in the conventional bureaucratic system. As a result, specific responses to cyber incidents may deviate from the strategic direction. Moreover, due to heightened threat perceptions on the other side, both sides will reduce restrictions on cyber operations, expand their operational scope, and increase the frequency of operations to obtain a greater sense of security in cyberspace.

3.3 The last but not the least challenge is how to reach a tacit agreement in cyberspace competition

Perhaps the lesson most frequently drawn from the crisis was the need to maintain lines of communication with the adversary, above all, at moments of greatest tension (Winham 1988, 22). Under the framework of the High-Level Joint Dialogue on Cybercrime and Related Issues from 2015 to 2017, the two sides discussed the first U.S.–China Senior Experts Group on International Norms in Cyberspace and Related Issues (U.S. Department of Justice 2016a) and launched the United States–China Cybercrime and Related Issues Hotline Mechanism (U.S. Department of Justice 2016b), which only addresses commercial cyber theft. The two militaries are not involved in the dialogue, due to the United States decision to charge the PLA officers, and neither does the dialogue cover broader issues in cyber conflicts.

Later, the United States Department of Justice pressed charges against Chinese institutions and businesses on cyber security grounds, which escalated rather than degraded the crisis, but these actions were deemed effective by US decision makers. To China, this was unacceptable and a blow to the foundation for cyber cooperation. Therefore, cybercrime remains the only area the two countries can work on at the moment.

According to Michael P. Fischerkeller, an American scholar involved in developing the strategy of "persistent engagement," cyberspace is a special space for strategic competition, which lies between the constraints of combat and combat operations, below the threshold of war. By means of a tacitly agreed upon competition, the competing parties could understand undefined, acceptable, or unacceptable competition behaviors in cyberspace and then carefully avoid actions commensurate with an armed attack while making an unspoken gentleman's agreement (Fischerkeller and Harknett 2019). However, the reality is that's not what U.S. policymakers want. In June 2019, the United States announced that it had placed malicious malware on Russia's power grid that could cause serious consequences to prevent selective blackouts in key Russian states during the 2020 election. At the end of 2020, the United States discovered that Russian hackers' cyberattacks, via the Solarwinds supply chain, had built the capability to strike critical infrastructure in the United States including electricity, energy, water, communications, and so on. The cyber contest between the United States and Russia has already shown that the United States cyber command's strategy of "persistent engagement" not only fails to bring about the strategic tacit understanding in cyberspace competition, but also urges the competitors to prepare for the "worst-case scenario."

If the United States continues to adopt ill-considered measures in its interactions with China, such as naming and shaming and maximum pressure, military facets of cyber-crisis management will be hardly covered in any meaningful arrangements, let alone reaching tacit understanding between the two sides.

4 Recommendations on promoting China–U.S. cooperation in cyber-crisis management

As two major powers in cyberspace, both China and the United States have a significant presence in this domain and regard it as a critical area. It is necessary that they strengthen cyber-crisis management to foster an environment of peace and trust as this would serve their own interests. In 2011, the United States released its first "International Strategy for Cyberspace," envisioning a future for cyberspace that is open, interoperable, secure, and reliable (The White House 2011). Similar ideas are also found in China's "International Strategy of Cooperation on Cyberspace" (The Ministry of Foreign Affairs and the Cyberspace Administration of China 2017). To prevent confrontation in the future, it is critical that China and the United States reach consensus on the basic principles of cyber-crisis management, open working channels, and identify clear goals so that there is space for them to avoid conflict and confrontation, find common ground, and accommodate each other.

4.1 First, build consensus on the basic principles of crisis management

The two sides still lack a basic consensus in the field of crisis management. This reflects the deep differences and deficiencies between the two sides in cyber strategic intention, cyber military security policy and communication mechanisms, which also hinders cooperation in cyber-crisis management.

Crisis management in cyberspace is an extension of crisis management. To achieve success, it needs to follow the basic rules of crisis management. Specifically, cyber-crisis management needs to adhere to the following four general principles. (1) The two sides should attach great importance to the most basic requirements of crisis management from the diplomatic level, including correctly understanding each other's interests and demands in cyberspace and accurately judging each other's intentions of cyber policy. (2) Each side should give the other a decent way to compromise, avoid naming, shaming, extreme pressure and other methods that lead to the accumulation and aggravation of contradictions, and ultimately run counter to the goal of solving the problem. (3) Avoid using force to deal with crises and rushing to issue ultimatums. Each side needs to give the other enough time to revise its policies, which means that both sides need to properly understand that cyber issues involve complex interagency coordination and that it is difficult to respond to each other's demands in a short period of time.4) Avoid dealing with crises on a zero-sum basis (Ding 2004, 32–35; Johnston 2016, 32).

In addition, since cybersecurity involves many fields, China and the United States also need to pay special attention to controlling the scope of the crisis in cyberspace

and preventing the crisis from spilling over into other fields. They should stay focused on the issues per se and prevent and minimize politicization and internationalization. In particular, among all the government agencies that may be involved in managing a crisis, the professional authorities that should play a leading role are those that bear the brunt of a crisis or have immediate interests involved. This is to prevent emotion-driven responses that may be counterproductive to the larger goal. Successful crisis management is an art of compromise, and past experiences show that a zero-sum mentality must be avoided.

4.2 Second, the role of academic exchange in crisis management should be brought into play

When crises happen, states tend to resort to confrontational measures to demonstrate determination, such as making representations, condemnations, recalling diplomatic representatives, and imposing sanctions. Formal channels of communication are thus partially closed. Therefore, it is important to diversify the communication mechanisms in peace times and have unimpeded civil channels when the normal channels are blocked.

Two mechanisms at the civil level have contributed to China–U.S. cyber-crisis management; namely, the China–U.S. Internet Forum and China–U.S. Cyber Security Track-2 Dialogue. The China–U.S. Internet Forum was jointly established by the Internet Society of China and Microsoft of the United States in 2007, aiming at promoting the exchange and cooperation between the internet industries of the two countries. The China–U.S. Cyber Security Track-2 Dialogue was launched by the China Institute of Contemporary International Relations and the Center for Strategic and International Studies of the United States in 2009. It has become an important platform for the academic and strategic research communities of the two countries to share their concerns.

If academic institutions and scholars of China and the United States can conduct in-depth exchanges and joint research on points of disagreement in peacetime, it will not only help to gain a deeper understanding of the contradictions, concerns, and consensus of the two sides, but also to identify feasible and operational suggestions for their respective policymaking, and more importantly, to promote bilateral, political, tacit understanding and benign interaction at the decision-making level and lay a foundation for bilateral cooperation in crisis management (Xu 2018). China and the United States have differences and contradictions in cyberspace, as well as common understandings and interests. The two sides need and can find a way to achieve competitive coexistence in cyberspace. Can China and the United States return to the six-point consensus on cybersecurity cooperation reached in 2015? Can China and the United States identify the agenda items they are willing to cooperate on, based on the 11 voluntary, non-binding codes of responsible conduct of states reached in the report of the United Nations Governmental Group of Experts on Information Security in 2015? These are areas that need to be studied and discussed jointly by the Chinese and American academic circles.

4.3 Third, confidence-building measures should be taken

Confidence-building measures can be taken to increase mutual trust and reduce the intensity of bilateral confrontation. These could be either military or non-military, and in either unilateral or bilateral form. For example, the policy recommendation of the Cyberspace Solarium Commission about reviewing "the defend forward concept and the delegation of authorities for offensive cyber operations" (King and Gallagher 2021, 11) is a constructive proposal that will help prevent cyber operations from escalating to a cyber crisis.

Regarding military confidence-building measures, given the common interest in preventing escalatory cyber operations, the two sides could consider conducting formal discussions on acceptable norms of behavior and possible thresholds for use of force as well as greater transparency on doctrine (Segal 2015). What's more, considering that the two militaries have signed the Memorandum of Understanding on Notification of Major Military Activities Confidence-Building Measures Mechanism and the Memorandum of Understanding Regarding the Rules of Behavior for Safety of Air and Maritime Encounters since 2014, which is major breakthrough for the two countries to build military confidence, the two sides may supplement the memoranda with annexes on cyber security crisis notification and rules of behavior for safety in cyberspace (Chen and Lu 2021, 6). In a multilateral framework, China and the United States could discuss and jointly promote an international agreement prohibiting the United States from initiating cyberattacks on nuclear weapons, taking into account the risks that information and communication technology pose to the nuclear field (Levite et al. 2021).

For confidence-building measures in non-military fields, since maintaining the openness, peace and security of cyberspace is in the common interest of China and the United States, the two sides can strengthen cooperation through the protection of international critical infrastructure, on which the global economy is highly dependent. If global financial information infrastructure, such as the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system, is damaged, it will bring a huge shock to the global economy. Preventing this could be the starting point for China–U.S. cooperation and trust-building in cyberspace. For another example, in the era of the global interconnection of everything, vulnerabilities have become an important cybersecurity risk affecting a country's economic development, national economy, and people's livelihoods, as well as a difficult problem in cyberspace governance. In response to the original problem of cybersecurity, aiming to eliminate potential threats to ICT and infrastructure that rely on China and the United States can jointly promote the international community to build a mutually beneficial and stable international mechanism for vulnerability management, which could be a breakthrough to implement responsible cyberspace codes of conduct, and the basis for building trust among cyberspace countries.

Declaration

Conflict of interest The authors declare that there is no competing interest regarding the publication of this article.

References

Brannen, Samuel J., Christian S. Haig, Katherine Schmidt, and Kathleen H. Hicks. 2020. Twin pillars: Upholding national security and national innovation in emerging technologies governance. CSIS. https://www.csis.org/analysis/twin-pillars-upholding-national-security-and-national-innovation-emerging-technologies. Accessed 6 April 2021.

BBC. 2015. Obama: China cyberattacks 'unacceptable'. https://www.bbc.com/news/world-us-canada-34229439. Accessed 15 May 2021.

Blanchard, Ben. 2015. China passes controversial counter-terrorism law. *Reuters*. https://www.reuters.com/article/us-china-security-idUSKBN0UA07220151228. Accessed 15 May 2021.

Campbell, Caitlin, and Craig Murray. 2013. China seeks a "new type of major-country relationship" with the United States. https://www.uscc.gov/sites/default/files/Research/China%20Seeks%20New%20Type%20of%20Major-Country%20Relationship%20with%20United%20States_Staff%20Research%20Backgrounder.pdf. Accessed 6 April 2021.

Central Committee General Office of China. 2016. Outline of the national informatization development strategy. https://chinacopyrightandmedia.wordpress.com/2016/07/27/outline-of-the-national-informatization-development-strategy/. Accessed 15 May 2021.

China Internet Network Information Center (CNNIC). 2008. The number of Chinese internet users exceed the US for the first time. *Beijing Daily*. https://it.sohu.com/20080725/n258380068.shtml. Accessed 19 May 2021.

Congressional Research Service. 2021. Renewed great power competition: Implications for defense—issues for Congress. https://crsreports.congress.gov/. Accessed 6 April 2021.

Chen, Dongxiao, and Chuanying Lu. 2021. Competition without catastrophe: A new China-U.S. cyber security agenda. Shanghai Institutes for International Studies. http://www.siis.org.cn/Research/EnInfo/5259. Accessed 6 April 2021.

Ding, Bangquan. 2004. *International crisis management*. Beijing: National Defense University Press.

Doshi, Rush, and Kevin Mcguiness. 2021. Huawei meets history: great powers and telecommunications risk: 1840–2021. https://www.brookings.edu/wp-content/uploads/2021/03/Huawei-meets-history-v4.pdf. Accessed 15 May 2021.

Dunsmuir, Lindsay. 2015. U.S. charges six Chinese nationals with economic espionage. *Reuters*. https://www.reuters.com/article/us-usa-china-theft-idUSKBN0O41PP20150520. Accessed 15 May 2021.

Finkle, Jim. 2013. Mandiant goes viral after China hacking report. *Reuters*. https://www.reuters.com/article/net-us-hackers-virus-china-mandiant-idUSBRE91M02P20130223. Accessed 6 April 2021.

Finklea, Kristin, Eric A. Fischer, Susan V. Lawrence, and Catherine A. Theohary. 2015. Cyber intrusion into U.S. Office of Personnel Management: In brief. *Congressional Research Service*. https://digital.library.unt.edu/ark:/67531/metadc743551/m1/1/high_res_d/R44111_2015Jul17.pdf. Accessed 15 May 2021.

FireEye Labs. 2015. APT 30 and the mechanics of a long-running cyber espionage operation. https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf. Accessed 15 May 2021.

Fischerkeller, Michael P., and Richard J. Harknett. 2019. Through persistent engagement, the U.S. can influence 'agreed competition'. *Lawfare*. https://www.lawfareblog.com/through-persistent-engagement-us-can-influence-agreed-competition. Accessed 15 May 2021.

Gass, Nick. 2015. Susan Rice headed to China later this week. *Politico*. https://www.politico.com/story/2015/08/susan-rice-to-china-121714. Accessed 15 May 2021.

George, Alexander L. (ed.). 1991. *Avoiding war: Problems of crisis management*. Westview Press.

Johnston, Alastair Iain. 2016. The evolution of interstate security crisis-management theory and practice in China. *Naval War College Review* 69(1): 28–71.

King, Angus, and Mike Gallagher. 2021. Cyberspace Solarium Commission white paper #5: Transition book for the incoming Biden administration. https://www.solarium.gov/public-communications/transition-book. Accessed 6 April 2021.

Levite, Ariel E., Jinghua Lyu, George Perkovich, Chuanying Lu, Manshu Xu, Bin Li, and Fan Yang. 2021. China-U.S. cyber-nuclear C3 stability. Carnegie and the Shanghai Institute for International Studies. https://carnegieendowment.org/files/Levite_et_all_C3_Stability.pdf. Accessed 10 May 2021.

Lu, Chuanying. 2014. Challenges facing the Obama administration's cyberspace strategy and its adjustment. *Contemporary International Relations* 5: 54–60.

Lu, Chuanying. 2019. Cyber security dilemma in China-US relations and its implications. *Contemporary International Relations* 12: 20–21.

Lu, Chuanying. 2020. Return of conservatism and repositioning of the Trump administration cyber security strategy. *World Economics and Politics* 1: 67–68.

Lynch III, Thomas F. (ed.). 2020. *Strategic assessment 2020: Into a new era of great power competition*. Washington, DC: National Defense University Press. https://ndupress.ndu.edu/Portals/68/Documents/Books/SA2020/Strategic-Assessment-2020.pdf?ver=-NTckVdG56-CfFYJ73PTgg%3d%3d. Accessed 15 May 2021.

Lyu, Jinghua. 2019. Keeping China–U.S. cyber conflict off the cards. https://carnegieendowment.org/2019/01/11/keeping-china-u.s.-cyber-conflict-off-cards-pub-78124. Accessed 6 April 2021.

Menn, Joseph. 2014. Private U.S. report accuses another Chinese military unit of hacking. *Reuters*. https://www.reuters.com/article/idUSL2N0OQ25L20140610. Accessed 15 May 2021.

Ministry of Foreign Affairs of China. 2015a. Xi Jinping gives interview to'The Wall Street Journal', emphasizing building new model of major-country relationship between China and US and enhancing peace, stability and development in Asia-Pacific region and world. https://www.fmprc.gov.cn/mfa_eng/topics_665678/xjpdmgjxgsfwbcxlhgcl70znxlfh/t1299819.shtml. Accessed 15 May 2021.

Ministry of Foreign Affairs of China. 2015b. Xi Jinping attends and addresses welcome banquet co-hosted by Washington State government and friendly groups of the US. https://www.fmprc.gov.cn/mfa_eng/topics_665678/xjpdmgjxgsfwbcxlhgcl70znxlfh/t1300269.shtml. Accessed 15 May 2021.

Ministry of Foreign Affairs of China. 2015c. Xi Jinping meets with main representatives from China and US who attends China-US internet industry forum, emphasizing China's advocacy of building peaceful, secure, open and cooperative cyberspace. https://www.fmprc.gov.cn/mfa_eng/topics_665678/xjpdmgjxgsfwbcxlhgcl70znxlfh/t1301069.shtml. Accessed 15 May 2021.

Ministry of Foreign Affairs of China. 2015d. Xi Jinping emphasizes strengthening China-US strategic mutual trust and pushing for continuous development of new model of China-US major-country relationship when meeting with President Barack Obama of the US. https://www.fmprc.gov.cn/mfa_eng/topics_665678/xjpdmgjxgsfwbcxlhgcl70znxlfh/t1302387.shtml. Accessed 15 May 2021.

Ministry of Foreign Affairs of China. 2015e. Full text: Outcome list of President Xi Jinping's state visit to the United States. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml. Accessed 15 May 2021.

Mölling, Christian. 2008. Comprehensive approaches to international crisis management. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-42.pdf. Accessed 6 April 2021.

Nakashima, Ellen. 2015. U.S. developing sanctions against China over cyberthefts. *Washington Post*. https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html. Accessed 6 April 2021.

Office of the Spokesperson of the United States. 2013. U.S.-China strategic and economic dialogue outcomes of the strategic track. https://2009-2017.state.gov/r/pa/prs/ps/2013/07/211861.htm. Accessed 6 April 2021.

Rasser, Martijin, and Megan Lamberth. 2021. Taking the helm: A national technology strategy to meet the China challenge. Center for a New America Security. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Taking-the-Helm_FINAL-compressed.pdf?mtime=20210113105310&focal=none. Accessed 15 May 2021.

Reuters. 2015. U.S., Chinese officials meet on cyber security issues: White House. https://www.reuters.com/article/idUSKCN0RC0S420150913. Accessed 15 May 2021.

Samenow, Jason, and Lisa Rein. 2014. Chinese hack U.S. weather systems, satellite network. *The Washington Post*. https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html. Accessed 15 May 2021.

Segal, Adam. 2015. Stabilizing cyber security in the U.S.-China relationship. *The National Bureau of Asian Research (NBR) Report*. https://www.nbr.org/publication/stabilizing-cybersecurity-in-the-u-s-china-relationship/. Accessed 6 April 2021.

Tang, Lan. 2021. Analyze the Biden administration's "cyber security concept" from the policy evolution. *China Information Security* 2: 77–80.

Tang, Lan, and Adam Segal. 2016. Reducing and managing U.S.-China conflict in cyberspace. *The National Bureau of Asian Research (NBR) Special Report*. https://www.nbr.org/wp-content/uploads/pdfs/publications/special_report_57_us-china_april2016.pdf. Accessed 6 April 2021.

The Atlantic Council. 2021. The longer telegram: Toward a new American China policy. https://www.wita.org/atp-research/new-american-china-strategy/. Accessed 6 April 2021.

The Ministry of Foreign Affairs and the Cyberspace Administration of China. 2017. International strategy of cooperation on cyberspace. *China Daily*. http://www.chinadaily.com.cn/opinion/2017-03/02/content_28401127.htm. Accessed 6 April 2021.

The State Council Information Office of the People's Republic of China. 2019. Full text: China's national defense in the new era. http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html. Accessed 16 June 2021.

The White House. 2011. International strategy for cyberspace. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Accessed 6 April 2021.

The White House. 2013. Remarks by President Obama and President Xi Jinping of the People's Republic of China after bilateral meeting. https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-. Accessed 9 May 2021.

Thomas, Elizabeth. 2016. US-China relations in cyberspace: The benefits and limits of a realist analysis. https://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/. Accessed 15 May 2021.

Thornhill, John. 2020. China is setting itself up to win cold war 2.0. *Financial Times*. https://www.ft.com/content/b6c5558e-ba0e-4381-b2b4-1acceb2ab484. Accessed 15 May 2021.

Trimintzios, Panagiotis, Roger Holfeldt, Mats Koraeus, Baris Uckan, Razvan Gavrila, and Georgios Makrodimitris. 2014. Report on cyber crisis cooperation and management: Comparative study on the cyber crisis management and the general crisis management. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/ccc-study. Accessed 15 May 2021.

U.S. Cyber Command. 2018. Achieve and maintain cyberspace superiority: Command vision for US cyber command. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf. Accessed 6 April 2021.

U.S. Department of Justice. 2015. First U.S.-China high-level joint dialogue on cybercrime and related issues summary of outcomes. https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0. Accessed 15 May 2021.

U.S. Department of Justice. 2016a. Second U.S.-China cybercrime and related issues high level joint dialogue. https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue. Accessed 15 May 2021.

U.S. Department of Justice. 2016b. Third U.S.-China high-level joint dialogue on cybercrime and related issues. https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues. Accessed 15 May 2021.

U.S. Joint Chiefs of Staff. 2018. Joint publication 3–12: Cyberspace operations. https://fas.org/irp/doddir/dod/jp3_12.pdf. Accessed 2 June 2021.

U.S. National Security Commission on Artificial Intelligence. 2021. Final report: National Security Commission on artificial intelligence. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf. Accessed 15 May 2021.

Wang, Xiaofeng. 2016. Causes of conflict and adjustment path of disputes over economic cyber espionage between China and the US. *American Studies* 5: 85–110.

Williams, Phil. 1976. *Crisis management: Confrontation and diplomacy in the nuclear age*. Martin Robertson & Co. Ltd.

Winham, Gilbert R. (ed.). 1988. *New issues in international crisis management*. Westview Press.

Wong, Edward. 2015. National security adviser meets with Chinese President before his U.S. visit. *The New York Times*. https://www.nytimes.com/2015/08/29/world/asia/susan-rice-xi-jinping-china.html. Accessed 15 May 2021.

Xi, Jinping. 2017. Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with Chinese characteristics for a new era. Delivered at the 19th National Congress of the Communist Party of China, 18 October 2017. http://www.chinadaily.com.cn/interface/flipboard/1142846/2017-11-06/cd_34188086.html. Accessed 15 May 2021.

Xu, Manshu. 2018. Recommendations for promoting cyber stability between China and the US. *Information Security and Communications Privacy* 6: 25–28.

Yayboke, Erol, and Sam Brannen. 2020. Promote and build a strategic approach to digital authoritarianism. CSIS. https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism. Accessed 6 April 2021.